UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
Northern Division

MARK EMERY, individually and on behalf of all others similarly situated,

Plaintiff

v.

KELLY & ASSOCIATES INSURANCE GROUP, INC. d/b/a KELLY BENEFITS
1 Kelly Way
Sparks, Maryland 21152

Serve On: Registered Agent
Steven I. Batoff, Esq.
Batoff Associates, P.A.
909 Saint Paul Street
Baltimore, MD 21202

and

AMERGIS HEALTHCARE STAFFING, INC.
7223 Lee Deforest Drive
Columbia, Maryland 21046

Serve On: Registered Agent
CSC-Lawyers Incorporating Service Co.
7 St. Paul Street – Suite 820
Baltimore, Maryland 21202,

Defendants.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Case No.:

Plaintiff Mark Emery ("Plaintiff") brings this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class Members") against Kelly & Associates Insurance Group, Inc. d/b/a Kelly Benefits ("Kelly Benefits") and Amergis Healthcare Staffing, Inc. ("Amergis" and, collectively with Kelly Benefits, "Defendants"), and alleges as follows, based upon information and belief, the investigation of counsel, and the personal knowledge of Plaintiff.

NATURE OF THE CASE

1. This "hub-and-spoke" data breach case involves the unauthorized access and exfiltration of the sensitive Personal Identifiable Information (PII), including financial account information, of over 413,000 Class Members, including Plaintiff.

2. The hub in this case is Defendant Kelly Benefits, one of the nation's largest providers of benefits administration and technology, broker and consulting services, and payroll solutions. During the ordinary course of its business, Kelly Benefits stores an enormous amount of PII and generated $4.3 billion in revenue last fiscal year.

3. One of the spokes surrounding Kelly Benefits is Defendant Amergis. Amergis is a national healthcare staffing company with over $2.4 billion in annual revenue.

4. Amergis is a customer of Kelly Benefits that used its services and software, and in doing so, entrusted Kelly Benefits with the PII of its customers and employees. The volume of PII stored by Amergis on Kelly Benefits' systems and platform was enormous and, according to Kelly Benefits' Data Breach Notice, included a broad array of sensitive PII, including Social Security numbers, tax ID numbers, dates of birth, medical information, health insurance information, financial account information, and other sensitive, identifying information.

5. Over a period of multiple days, in December 2024, cybercriminals infiltrated Kelly Benefits' network and exfiltrated the PII of over 413,000 individuals stored by Kelly Benefits' customers on Kelly Benefits systems and platform (the "Data Breach").

6. Kelly Benefits' forensic investigation to date has not publicly revealed how cybercriminals gained unauthorized exposure to Kelly Benefits' network and systems but it is clear the Data Breach occurred because Kelly Benefits and Amergis failed to implement fundamental and basic security measures that could have prevented the Data Breach.

7. Plaintiff and Class Members have been substantially injured by Defendants' data security failures. Plaintiff further believes that he and Class Members' Private Information has or will be published for sale on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

8. As a result of the Data Breach, Plaintiff has suffered numerous injuries, including invasion of privacy, lost time and expenses mitigating the risk of data misuse, the diminishment in value of his PII, and failing to receive the benefit of the bargain reached with Defendants.

9. Plaintiff brings this action to hold Defendants accountable for their data security failures, enjoin their continued failure to implement basic and fundamental data security practices, and recover damages and all other relief available at law on behalf of himself and members of the classes he seeks to represent.

PARTIES

A. Defendant

10. Defendant Kelly Benefits is a privately held insurance company specializing in human resources and benefits administration with its headquarters and principal place of business in Baltimore County. Kelly Benefits is a for-profit company organized and incorporated under its parent company, Kelly Services, Inc., under the laws of the State of Delaware.

11. Because Defendant Kelly Benefits has its headquarters and principal place of business in the State of Maryland, Defendant Kelly Benefits is a citizen of the States of both Maryland and Delaware.

12. Defendant Amergis is headquartered and has its principal place of business in Columbia, Maryland, in Howard County. Amergis has locations across the country.

13. Because Defendant Amergis is headquartered and has its principal place of business

in Columbia, Maryland Amergis is a citizen of Maryland.

14. Defendant Amergis is a customer of Defendant Kelly Benefits and, on information and belief, used Kelly Benefits' compromised software.

B. Plaintiff

15. Plaintiff Mark Emery is a Pittsburgh, Pennsylvania resident of Allegheny County, who is a former employee of Defendant Amergis.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members, including Plaintiff Emery, are citizens of a different state than *any* Defendant. Specifically, Plaintiff Emery is a citizen of the State of Pennsylvania and, Defendant Kelly Benefits is a citizen only of the States of Maryland and Delaware, and Defendant Amergis is a citizen of Maryland.

17. This Court has personal jurisdiction over Defendants because Defendants maintain their headquarters and principal places of business in this District. Defendants also conduct substantial business in this District, engaged in the conduct at issue in this District, and/or otherwise have substantial contacts with this District and purposely availed themselves of the Courts in this District.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(1)-(2), 1391(b)(2), and 1391(c)(2) as Defendants' principal places of business are in this District and a substantial part of the events giving rise to the claims emanated from activities within this District.

FACTUAL ALLEGATIONS

I. Kelly Benefits' Business

19. Kelly Benefits is a privately held insurance company founded in 1976. Kelly Benefits is best known for its human resources and benefits administration.

20. Kelly Benefits touts its ability to seamlessly connect its customers' "current systems with Kelly Benefits' Total Benefits Solution® technology" to provide "a full suite of integrated business solutions."[1]

21. Kelly Benefits' proprietary Total Benefits Solution® technology ("KTBSonline") "offers a single point of entry for brokers, employers and employees" and "was designed by brokers and consultants with hundreds of years of combined experience in understanding the complexity and challenges of employee benefits management."[2]

22. Each of Kelly Benefits' customers, including Defendant Amergis, stores PII of their customers and/or employees on Kelly Benefits' platform through the use of Kelly Benefits' offered services and software.

23. Kelly Benefits' marketing demonstrates that it is well-aware that data security is a key component of the services it provides to its customers. The following examples illustrate how Kelly Benefits markets and highlights the strength of its data security practices to entice customers to use Kelly Benefits' products and services, as well as Kelly Benefits' awareness of industry guidance and regulations that set standards for effective data security practices:

---

[1] https://www.KellyBenefits.com/ (Last visited May 12, 2025).

[2] https://kellybenefits.com/resources/ktbsonline/#:~:text=KTBSonline%2C%20Kelly%20Benefits%27%20proprietary%20Total%20Benefits%20Solution%C2%AE,complexity%20and%20challenges%20of%20employee%20benefits%20management.&text=Client%20Database%20and%20Eligibility%20Management%20System:%20Benefit,secure%20electronic%20billing%20payment%20and%20management%20options (Last visited May 12, 2025).

- Kelly Benefits claims to "***maintain[] a robust information security program to ensure the protection and availability of our customers' sensitive data***. We have full-time Security Engineers on-staff and maintain relationships with a number of industry-leading security partners. With these partners, we conduct a comprehensive annual assessment and penetration test of our systems."[3]

- Kelly Benefits also claims that "[o]ur development environments only contain sanitized non-identifiable data, and our developers code against common attacks such as SQL injection."[4]

- Kelly Benefits also advertises several industry protocols it purports to support, maintain and be accredited in, including SOC1 Type II, SOC2 Type II, and the NIST 800-53 standards.[5]

- Kelly Benefits' Privacy Policy represents their "firm commitment to protecting user privacy and sensitive user information."[6]

- Kelly Benefits' Privacy Policy also represents that "[w]e use reasonable care to protect your data from loss, misuse, unauthorized access, disclosure, alteration and untimely destruction…***Please be assured that the Site is equipped with security measures to protect the information you provide us***. Kelly Benefits processes user information in a proper method and takes appropriate security measures to prevent unauthorized access, disclosure, modification, or unauthorized destruction of personal identifiable information."[7]

24. During the ordinary course of its business (primarily through the operation of its cloud-based databases and KTBSonline), Kelly Benefits receives the PII of individuals, such as Plaintiff and the Class, from Kelly Benefits' customers, including Defendant Amergis.

25. Because cloud-based databases and software applications like KTBSonline are prime targets for cybercriminals due to the sheer volume of data they house and transfer, Kelly Benefits should have known of the risks of a potential data breach. One recent report has

[3] https://kellybenefits.com/resources/ktbsonline/security/ (Last visited May 12, 2025).
[4] *Id.*
[5] *Id.*
[6] https://kellybenefits.com/privacy-policy/ (Last visited May 12, 2025).
[7] *Id.*

highlighted the risks presented specifically by cloud storage as follows:[8]

> It is estimated that more than 60% of the world's corporate data is stored in the cloud. ***That makes the cloud a very attractive target for hackers. In 2023, over 80% of data breaches involved data stored in the cloud***. That is not just because the cloud is an attractive target. In many cases, ***it is also an easy target due to cloud misconfiguration*** – that is, companies unintentionally misuse the cloud, such as allowing excessively permissive cloud access, having unrestricted ports, and use unsecured backups.

II. Amergis' Business

26. Defendant Amergis is a national healthcare staffing company with over 10,000 employees, serving clients across the country.[9] One of Amergis' primary business functions is to help its clients staff their healthcare workforces.

27. Like Kelly Benefits, Amergis is well-aware of the significance and necessity of data security to its customers and employees. Amergis' Privacy Policy highlights the importance of data security to its customers and employees, including stating that "[w]e maintain commercially reasonable security measures to protect the personal data we collect and store from loss, misuse, destruction, or unauthorized access."[10]

28. In the ordinary course of business, Defendant Amergis receives the PII of individuals, from its employees and the entities and individuals that utilize Amergis' services. In turn, Amergis entrusts this PII to its third-party vendors and service providers like Kelly Benefits.

29. Amergis is a Kelly Benefits customer. Amergis stores the PII of its employees and customers on Kelly Benefits' software, network, and/or products, and utilized KTBSonline.

---

[8] https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 (Last visited Apr. 16, 2025).
[9] https://www.linkedin.com/company/amergisstaffing/about/ (Last visited May 12, 2025).
[10] https://www.amergis.com/privacy-policy/ (Last visited May 12, 2025).

III. Amergis and Kelly Benefits obtain, collect, use, and derive a benefit from the PII of Plaintiff and Class Members.

30. Defendants obtain, collect, use, and derive a benefit from the PII of Plaintiff and Class Members. Defendants use this PII to provide services, making a profit therefrom. Defendants would not be able to obtain revenue if not for the acceptance and use of this PII.

31. By collecting Plaintiff's and the Class's PII, either directly or indirectly, Defendants assumed legal and equitable duties to Plaintiff and the Class to protect and safeguard their PII from unauthorized access and intrusion.

32. Defendants each recognize this duty in their respective Privacy Policies and marketing to their customers and employees.

33. Defendants' assurances of maintaining high standards of cybersecurity make it evident that Defendants recognized that they had a duty to use reasonable measures to protect the PII that they collected and maintained.

34. Defendants violated their own overt privacy statements and failed to adopt reasonable and appropriate security practices and procedures including administrative, physical security, and technical controls to safeguard Plaintiff's and Class Member's PII.

35. As a result, Plaintiff's and Class Members' PII was accessed and stolen from Defendants' inadequately secured data systems in a massive and preventable Data Breach.

IV. The Data Breach.

36. In December 2024, Kelly Benefits became aware that cybercriminals had exploited critical vulnerabilities in Kelly Benefits' network security, which allowed for unauthorized data access between December 12, 2024, and December 17, 2024.

37. Defendants have publicly acknowledged the Data Breach and provided notice of

the Data Breach to various State Attorneys General and some of the victims, including Plaintiff. Specifically, on April 9, 2025, Kelly Benefits began notifying States' Attorneys General of the Data Breach, initially confirming that over 32,000 individuals were impacted and claiming that the Data Breach was not discovered until March 3, 2025.[11] Then, on April 21, 2025, and May 2, 2025, Kelly Benefits provided supplemental notifications to States' Attorneys General of the Data Breach, including updating the number of individuals impacted by the Data Breach to 263,000, and again updating that figure to over 413,000.[12]

38. In April 2025, Kelly Benefits also began providing affected individuals Data Breach notification letters on behalf of their customers, including Defendant Amergis.

39. Defendants failed to take the necessary precautions required to safeguard and protect Plaintiff's and Class Members' PII from unauthorized access and exploitation. The risk of cyberattacks, such as occurred here, should have been well known to Defendants. Defendants could have taken, but did not take, many simple preventive measures to prevent the Data Breach.

40. Defendants' actions and inactions represent a flagrant disregard of the rights of Plaintiff and the Class.

V. Relevant Industry Standards and Regulations for Data Security

A. Federal Deposit Insurance Corporation

41. The United States Federal Deposit Insurance Corporation ("FDIC") has issued guidance concerning implementation and compliance with its "Privacy Rule," which is meant to

[11] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/047b774f-2e79-4a04-9f4c-4dd7a8b2ee8d.html (Last visited May 12, 2025).
[12] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/31cc467f-60ce-43da-985b-1157966dc553.html; and https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/7a0c076f-6530-433d-b017-bb849c81b4b8.html (Last visited May 12, 2025).

protect consumers' PII and "governs when and how banks may share nonpublic personal information about consumers with nonaffiliated third parties."[13]

B. United States Federal Trade Commission Guidelines

42. The United States Federal Trade Commission ("FTC") has issued numerous forms of guidance and taken enforcement actions that outline the data security industry standards applicable to Defendants.

43. For example, the FTC's enforcement actions have established that a company's failure to maintain reasonable and appropriate data security of consumer PII violates the FTC Act's prohibition on "unfair or deceptive acts."[14]

44. In 2016, the FTC published guidance entitled *Protecting Personal Information: A Guide for Business* (the "FTC 2016 Guidance"). The FTC 2016 Guidance:

- Stresses the importance of "[c]ontrol[ling] access to sensitive information" and expressly encourages businesses to "[c]onsider using multi-factor authentication, such as requiring the use of a password and a code sent by different methods."[15]

- Emphasizes that companies should respond appropriately when credentials are compromised, providing that businesses should "[r]equire password changes when appropriate—for example, following a breach."

- Instructs companies to restrict data access privileges by "[s]cal[ing] down access to data" and ensuring that "each employee should have access only to those resources needed to do their particular job."[16]

- Warns companies that their data security practices depend on their personnel, which "includ[e] contractors" and encourages companies to "investigate [contractor] data security practices and compare their

[13] *See* https://www.fdic.gov/bank-examinations/privacy-rule-handbook (Last visited Apr. 16, 2025).
[14] *See, e.g., In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F.Supp.3d 374, 407 (E.D. Va. 2020) (citing *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)).
[15] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (Last visited Apr. 16, 2025).
[16] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (Last visited Apr. 16, 2025).

standards" and "verify compliance" with written security expectations.

- Recommends companies encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems and respond to security incidents.

- Advises companies not to maintain PI longer than necessary, not to collect more PI than necessary, to use industry-tested methods for data security, and monitor and respond to suspicious activity.

45. In 2021, the FTC amended its "Safeguards Rule" that applies to financial institutions, including retailers that issue their own credit cards to consumers and companies that bring together buyers and sellers of products and services.[17] The Safeguard Rule expressly requires covered businesses to "[i]mplement multi-factor authentication for anyone accessing customer information on [the business's] system," to "[i]mplement and periodically review access controls [to] [d]etermine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it," and "[i]mplement procedures and controls to monitor when authorized users are accessing customer information on your system and detect unauthorized access."[18]

46. In February 2023, the FTC published an article entitled *Security Principles: Addressing underlying causes of risk in complex systems.* The article highlighted the importance of MFA, stating: "Multi-factor authentication is widely regarded as a critical security practice because it means a compromised password alone is not enough to take over someone's account."[19]

C. Data Breaches Are Preventable

47. Despite the growing body of publicly available information regarding the rise of

[17] 16 C.F.R. §§ 314.2(h)(2)(i), (xiii).
[18] *See* https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (Last visited Apr. 16, 2025).
[19] *See* https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems (Last visited Apr. 16, 2025).

ransomware attacks and other forms of cyberattacks that compromise PII, Defendants' approach to maintaining the privacy of Plaintiff's and Class Members' PII was inadequate, unreasonable, negligent, and reckless. Defendants failed to use reasonable security procedures and practices appropriate to the nature of the sensitive information Defendants were maintaining and transferring for Plaintiff and Class Members such as encrypting the information or deleting it when it is no longer needed, and this caused the exposure of PII.

48. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[20]

49. Defendants could have prevented this Data Breach. Defendants could have and should have implemented measures—as recommended by the United States Government—to prevent and detect cyberattacks and/or ransomware attacks, including, but not limited to, the following recommendations:

- **Implement an awareness and training program**. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- **Enable strong spam filters** to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- **Scan all incoming and outgoing emails** to detect threats and filter executable files from reaching end users.
- **Configure firewalls** to block access to known malicious IP addresses.
- **Patch operating systems, software, and firmware on devices**. Consider using a centralized patch management system.
- **Set anti-virus and anti-malware programs to conduct regular scans**

[20] Ransomware Prevention and Response, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (Last visited Apr. 16, 2025).

automatically. Ensure these programs run automatic scans to detect and remove potential threats.

- **Manage the use of privileged accounts based on the principle of least privilege**: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- **Configure access controls**—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- **Disable macro scripts from office files transmitted via email**. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- **Implement Software Restriction Policies (SRP)** or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- **Disable Remote Desktop protocol (RDP)** if it is not being used.

- **Use application whitelisting**, which only allows systems to execute programs known and permitted by security policy.

- **Execute operating system environments or specific programs in a virtualized environment**. Run sensitive systems or programs in isolated virtual environments to reduce risk.

- **Categorize data based on organizational value** and implement physical and logical separation of networks and data for different organizational units.[21]

50. To prevent and detect cyberattacks and ransomware attacks, Defendants could and should have implemented the following preventive measures, as recommended by Microsoft's Threat Protection Intelligence Team:

- **Secure internet-facing assets**

[21] *Id.*

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audits
- remove privileged credentials

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**

  - Ensure collaboration among security operations, security admins, and information technology admins to configure servers and other endpoints securely

- **Build credential hygiene**

  - Use multifactor authentication or network level authentication and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**

  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**

  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and Antimalware Scan Interface for Office Visual Basic for Applications.[22]

51. Similarly, Defendants could and should have implemented measures—as also recommended by the United States Government—to prevent and detect cyberattacks and/or ransomware attacks, including the following recommendations:

- Know what personal information you have in your files and on your computers.

[22] *See* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (Last visited Apr. 16, 2025).

- Keep only what you need for your business.
- Protect the information that you keep.
- Properly dispose of information you no longer need. Create a plan to respond to security incidents.[23]

52. Finally, Defendants could and should have implemented the following measures—as also recommended by the United States Government—to prevent and detect cyberattacks and/or ransomware attacks, including the following recommendations:

- **Conduct regular vulnerability scanning to identify and address vulnerabilities**, especially those on internet-facing devices, to limit the attack surface.

- **Regularly patch and update software and operating systems to the latest available versions.** Prioritize timely patching of internet-facing servers that operate software for processing internet data such as web browsers, browser plugins, and document readers-especially for known exploited vulnerabilities….

- **Limit the use of RDP and other remote desktop services.** If RDP is necessary, apply best practices. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later traverse the network using the native Windows RDP client.

- **Ensure all on-premises, cloud services, mobile, and personal devices are properly configured, and security features are enabled**. For example, disable ports and protocols that are not being used for business purposes.[24]

53. Given that Defendants were collecting, storing, and transferring highly sensitive PII belonging to Plaintiff and Class Members, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

54. The occurrence of the Data Breach indicates that Defendants failed to adequately

[23] *See* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (Last visited Apr. 16, 2025).
[24] *See* https://www.cisa.gov/resources-tools/resources/stopransomware-guide (Last visited Apr. 16, 2025).

implement one or more of the above measures to prevent cyberattacks or ransomware attacks, resulting in the Data Breach and data thieves accessing and acquiring the PII of Plaintiff and hundreds of thousands of Class Members.

D. Defendants Acquire, Collect, and Store Plaintiff's and Class Members' Private Information

55. Defendants acquire, collect, and store a significant amount of PII belonging to Class Members.

56. As a condition of engaging in services with Amergis, Plaintiff and Class Members were required to entrust their highly sensitive PII to Amergis, and in turn either directly or indirectly to Defendant Kelly Benefits.

57. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

58. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendants absent a commitment to safeguard that information.

59. Upon information and belief, while collecting PII from Plaintiff and Class Members, Defendants promised to provide confidentiality and adequate security for their data through their applicable privacy policies and through other disclosures in compliance with statutory privacy requirements.

60. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. The Data Breach occurred because Defendants failed to do so.

E. Value of Private Information

61. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[25] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[26]

62. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[27]

63. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information at the point-of-sale in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, Social Security numbers, or other government issued identification numbers.

64. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

65. The fraudulent activity resulting from the Data Breach may not come to light for

[25] 17 C.F.R. § 248.201 (2013).
[26] *Id.*
[27] *See* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (Last visited Apr. 16, 2025).

years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

66. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

F. Industry Standards Specific to Cloud Data Storage

67. In addition to the general data security standards described above, numerous authorities have issued guidance specific to cloud data storage, defining the roles and responsibilities of cloud service providers (like Kelly Benefits) and customers (like Amergis).

i. Governmental Authorities

68. In June 2020, the FTC published an article titled, *Six steps toward more secure cloud computing.* The article warned, "[a]s cloud computing has become business as usual for many businesses, frequent news reports about data breaches and other missteps should make companies think carefully about how they secure their data." The article expressly highlighted the importance of MFA in protecting consumer data stored on cloud services, recommending businesses: "Require multi-factor authentication and strong passwords to protect against the risk

[28] *See* https://www.gao.gov/assets/gao-07-737.pdf (Last visited Apr. 16, 2025).

of unauthorized access."[29]

69. In March 2023, the FTC issued a Request for Information seeking public comment on "Business Practices of Cloud Computing Providers that Could Impact Competition and Data Security."[30] After reviewing over 100 public comments on the issue, the FTC published a report in November 2023 titled, *Cloud Computing RFI: What we heard and learned*. The report expressly flagged the room for improvement in cloud security as follows: "[A] a number of commenters argued there is a great deal of room for improvement in cloud security; that default security configurations could be better; and that the "shared responsibility" model for cloud security often lacks clarity, which can lead to situations where neither the cloud provider nor the cloud customer implements necessary safeguards."[31]

70. In March 2024, the U.S. National Security Agency and Cybersecurity & Infrastructure Agency issued a joint publication titled, *Use Secure Cloud Identity and Access Management Practices.* The publication warned, "[a]s organizations continue to migrate to using cloud environments, these environments are becoming increasingly valuable targets for malicious cyber actors[.]" The publication made numerous recommendations relevant to MFA, rotating credentials, and restricting allow lists to ensure only necessary privileges are granted to users:

> - **Multifactor authentication.** Single-factor authentication (e.g., password or PIN only) based account access is susceptible to credential theft, forgery, and reuse across multiple systems. Cloud accounts are generally globally accessible; thus they are more susceptible to certain types of single-factor authentication weaknesses. Multifactor authentication (MFA) boosts

[29] https://www.ftc.gov/business-guidance/blog/2020/06/six-steps-toward-more-secure-cloud-computing (Last visited Apr. 16, 2025).
[30] https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-seeks-comment-business-practices-cloud-computing-providers-could-impact-competition-data (Last visited Apr. 16, 2025).

[31] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/11/cloud-computing-rfi-what-we-heard-learned (Last visited Apr. 16, 2025).

> account security, better resisting compromise by enhancing user verification methods. MFA requires two or more factors for login: something the user knows, has, or is. Typically this is implemented using a password and a second factor usually based on a randomly seeded numeric token, a biometric option (such as a fingerprint or facial recognition), or a physical token (unique hardware-based identifier: smartcard, Common Access Card, etc.).
>
> - Periodically audit IAM configurations to confirm only necessary privileges are granted to users. Many CSPs [Cloud Service Providers] offer services that will track unused privileges to help admins tailor accounts to the least privileges users need to accomplish their day-to-day responsibilities.

71. Also in March 2024, NSA separately issued a publication titled, *NSA's Top Ten Cloud Security Mitigation Strategies.* The publication emphasized the importance of MFA, credential rotation, and restricted allow lists as follows for customers using cloud data services as follows:[32]

> Proper identity and access management (IAM) are critical to securing cloud resources. Malicious actors can compromise accounts using phishing techniques, exposed credentials, or weak authentication practices to gain initial access into cloud tenants. They can also exploit overly broad access control policies to penetrate further into the environment, gaining access to sensitive resources. To prevent this, cloud users should use secure authentication methods such as phishing-resistant multifactor authentication (MFA) and properly managed temporary credentials. Access control policies should be carefully configured to ensure users are granted the least privileges necessary. Separation of duties should be implemented to protect especially sensitive operations and resources.

ii. **Industry Standards**

72. The PCI Data Security Council has issued an April 2018 supplement to the PCI DSS titled, *Cloud Computing Guidelines.*[33] The PCI Cloud Computing Guidelines again emphasize the importance of MFA, providing: "PCI DSS Requirement 8.2.2 requires multi-factor

[32] https://media.defense.gov/2024/Mar/07/2003407860/-1/-1/0/CSI-CloudTop10-Mitigation-Strategies.PDF (Last visited Apr. 16, 2025).
[33] https://listings.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf (Last visited Apr. 16, 2025).

authentication for all remote network access to the CDE [cardholder data environment], and when public cloud services are part of a Customer's CDE, all such access will be considered remote access and will require multi-factor authentication.

73. The PCI Cloud Computing Guidelines includes a section titled *Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)*, which provides: "As the Customer's access to network level data can be severely restricted in cloud environments, the responsibility for tracking intrusions at the network layer will often reside with the Provider, as the only entity that has sufficient privileges to do this across the underlying infrastructure." The guidelines go on to note that for SaaS providers such as Kelly Benefits: "Since customer access to low level network traffic is impossible, it must rely on Providers for IDS/IPS, monitoring and alerting."[34]

74. The Center for Internet Security ("CIS") is a non-profit organization that develops globally recognized best practices for securing IT systems and data. In March 2022, CIS issued a publication entitled *CIS Controls Cloud Companion Guide* that provided guidance as on security best practices for customers using cloud services. The guidance made the following recommendations emphasizing the importance of MFA and revoking access to stale credentials:

- **Disable Dormant Accounts.** Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.
- **Establish an Access Revoking Process.** Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.
- **Require MFA for Administrative Access.** Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.

[34] https://listings.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf (Last visited Apr. 16, 2025).

75. ISO/IEC 27017 is an international standard that "provides controls and implementation guidance for both cloud service providers and cloud service customers."[35] Control 9.2.3 specifically highlights that cloud service customers (like AMERGIS) should use MFA and cloud service providers (like Kelly Benefits) should provide MFA capabilities as follows:

Cloud service customer	Cloud service provider
The cloud service customer should use sufficient authentication techniques (e.g., multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service according to the identified risks.	The cloud service provider should provide sufficient authentication techniques for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service, according to the identified risks. For example, the cloud service provider can provide multi-factor authentication capabilities or enable the use of third-party multi-factor authentication mechanisms.

VI. Defendants Each Owed a Duty of Care to Plaintiff and Class Members.

76. The PII of Plaintiff and Class Members was stored on Defendants' platforms, networks, systems or products at the time of the Data Breach.

77. Defendants owed common law duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendants' possession from being compromised, accessed, stolen, or misused by unauthorized parties.

A. Defendant Kelly Benefits Breached its Duty of Care to Plaintiff and Class Members

78. Defendant Kelly Benefits' duty of reasonable care is established due to the nature of its business, which is to provide *secure* human resources and benefits administration via its

[35] https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027017-2015.pdf (Last visited Apr. 16, 2025).

proprietary KTBSonline software to customers, and store massive amounts of data, including Plaintiff's and Class Members' PII. In offering and undertaking these services to customers, Kelly Benefits had a duty to exercise reasonable care to safeguard Plaintiff's and Class Members' PII because it was foreseeable that failure to do so would cause them injury.

79. Kelly Benefits' duty of reasonable care is established by governmental regulations and industry guidance establishing industry standards for data security to safeguard the PII it stored.

80. Kelly Benefits' duty of reasonable care is also established by its own marketing statements and Privacy Policy, which hold out its secure provision of services.

81. Kelly Benefits' duty of reasonable care is also established by relevant common law.

82. Kelly Benefits breached its duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII by failing to implement adequate data security practices, which caused the Data Breach.

83. Kelly Benefits was negligent and breached its duty of care to Plaintiff and Class Members to protect their PII from exploitation via customers' use of KTBSonline.

84. Kelly Benefits' breach of its duty of care caused the Data Breach, because if Kelly Benefits had maintained adequate data security, the Data Breach could have been prevented.

85. Kelly Benefits' data security failings also constitute an unfair trade practice. As discussed above, the FTC's enforcement actions have established that a company's failure to maintain reasonable and appropriate data security of PII violates the FTC Act's prohibition on "unfair and deceptive acts."

86. Kelly Benefits' breach of its duty of care and engagement in unfair trade practices caused injury to Plaintiff and Class Members.

87. Kelly Benefits is liable for the injuries suffered by Plaintiff and Class Members by virtue of its role as the proprietary owner and administrator of KTBSonline, which was used to facilitate the transfer of and store the data of its affected customers, including Defendant Amergis.

B. Defendant Amergis Breached its Duty of Care to Plaintiff and Class Members

88. At the time of the Data Breach, Amergis failed to maintain reasonable data security measures and comply with FTC guidance and other relevant industry standards. These data security failings included: Amergis' failure to adequately oversee or select third party vendors to which it entrusted the PII of its consumers and employees.

89. Amergis' data security failings enabled the Data Breach. Without these basic protections, cybercriminals were able to exfiltrate the PII of Plaintiff and Class Members.

90. Amergis, through these basic data security failings, breached its express representations in its Privacy Policy, detailed earlier in the complaint.

91. In the alternative, Amergis breached implied commitments to protect the PII of customers and employees, including Plaintiff and Class Members, by virtue of mandating that customers and employees provide their sensitive PII as a condition of utilizing Amergis' services and/or employment with Amergis.

92. Amergis' basic data security failings also constitute a breach of its duty of care to protect the PII of customers and employees, which include Plaintiff and Class Members.

C. Plaintiff and Class Members have suffered injuries as a result of the Data Breach.

93. Plaintiff and Class Members have suffered the following forms of injury as a result of the Data Breach.

94. The Data Breach's disclosure of Plaintiff's and Class Members' PII has created a

substantial risk that their data will be misused. This risk is demonstrated by the fact that cybercriminals now control that data.

95. Plaintiff and Class Members have reasonably expended significant time and costs mitigating against the substantial risk of data misuse. These mitigation steps include that Plaintiff and the Class must now take the time and effort to place "freezes" and "alerts" with credit reporting agencies, contact their financial institutions, close or modify financial accounts, and closely review and monitor bank accounts and credit reports for unauthorized activity for years to come.

96. Plaintiff and Class Members also suffered lost property value in their PII when Defendants allowed their PII to fall into the hands of cybercriminals, which in all likelihood will freely sell or distribute their PII at any time.

97. Amergis breached its express and implied contractual commitments to Plaintiff and Class Members to protect their PII.

98. The breach of a contractual obligation constitutes an injury to Plaintiff and Class Members and provides a basis for a lawsuit to enforce the terms of the contract.

99. In breaching their contractual commitments, Amergis further injured Plaintiff and Class Members by depriving them of the benefit-of-the-bargain they had reached.

100. For example, Plaintiff and Class Members entered into agreements with Amergis based on express and implied representations that their PII would be protected—which was factored into the value of that exchange. As Amergis failed to maintain reasonable data security measures to protect that PII, they deprived Plaintiff and Class Members of the benefit-of-the-bargain where they were owed the value of reasonable data security measures that were not provided.

101. Plaintiff and Class Members have also been injured by an invasion of their privacy

rights. The disclosure of their PII to cybercriminals and potentially others if and when the cybercriminals disclose it on the web involves PII whose private nature was compromised by the Data Breach.

102. In addition, Plaintiff and Class Members have suffered emotional distress and anxiety resulting from the Data Breach and fearing the substantial risk of identity theft and loss of privacy. Plaintiff and Class Members understand that their PII cannot now be clawed back from the Dark Web.

VII. Plaintiff Emery's Individual experience

103. Plaintiff Emery is a former employee of Defendant Amergis who served as a recruiter on behalf of Defendant Amergis.

104. Upon information and belief Plaintiff's PII was stolen from Defendants' systems, networks, and/or software in the Data Breach.

105. Defendants were in possession of Plaintiff's PII before, during, and after the Data Breach.

106. Because of the Data Breach, Plaintiff Emery's confidential PII is in the hands of cybercriminals. As such, Plaintiff Emery and other Class Members are at imminent risk of identity theft and fraud.

107. As a result of the Data Breach, Plaintiff Emery must expend hours of his time and suffered loss of productivity addressing and attempting to ameliorate, and mitigate, the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information.

108. Plaintiff Emery places significant value on the security of his PII and does not

readily disclose it. Plaintiff Emery has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

109. Plaintiff Emery has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII compromised by the Data Breach.

110. Plaintiff Emery has a continuing interest in ensuring that his PII, which, upon information and belief, remains in the possession of Defendants, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff's and the Class's PII will be wholly unprotected and at-risk of future data breaches.

111. Plaintiff suffered actual injury as a result of the unauthorized access and disclosure of his PII in the Data Breach including, but not limited to: (i) invasion of privacy; (ii) disclosure and/or theft of his PII; (iii) lost or diminished value of his PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) nominal damages; and (vi) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect his PII.

112. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not informed Plaintiff of key details about the Data Breach's occurrence.

VIII. Class Action Allegations

113. Plaintiff brings this action on his own behalf, and on behalf of the following "Kelly

Benefits Class":

> **Kelly Benefits Class.** All individuals residing in the United States whose PII was identified as compromised in the Data Breach.

114. Plaintiff's proposed class definitions against Kelly Benefits are inclusive of proposed national and state class definitions against Amergis. For example, the Kelly Benefits Class includes the Class proposed for Amergis.

115. Plaintiff also brings this action on his own behalf, and on behalf the following "Amergis Class":

> **Amergis Class.** All current and former Amergis customers and employees residing in the United States whose data was accessed or stolen in the Data Breach.

116. Excluded from the Kelly Benefits Class and the Amergis Class are Kelly Benefits' and Amergis' officers, directors, and any entity in which Kelly Benefits and Amergis has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Kelly Benefits and Amergis. Excluded also from the Kelly Benefits Class and Amergis Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

117. Plaintiff reserves the right to amend or modify the definition of the Kelly Benefits Class and Amergis Class or create additional subclasses as this case progresses.

118. **Numerosity.** The members of the Kelly Benefits Class and Amergis Class are so numerous that joinder of all of them is impracticable. Public reporting presently indicates that there are over 20 companies, with over 400,000 customers, whose data was implicated in the Data Breach.

119. **Commonality.** There are questions of fact and law common to the Kelly Benefits Class and Amergis Class, which predominate over individualized questions. These common

questions of law and fact include, but are not limited to:

- Whether Kelly Benefits and Amergis had a duty to protect the PII of Plaintiff and Kelly Benefits Class and Amergis Class Members, and whether they breached that duty.
- Whether Kelly Benefits and Amergis knew or should have known that their data security practices were deficient.
- Whether Kelly Benefits' and Amergis' data security systems were consistent with industry standards prior to the Data Breach.
- Whether Plaintiff and Kelly Benefits Class and Amergis Class Members are entitled to actual damages, punitive damages, treble damages, statutory damages, nominal damages, and/or injunctive relief.

120. **Typicality.** Plaintiff's claims are typical of those of other Kelly Benefits Class and Amergis Class Members because Plaintiff's PII, like that of every other Kelly Benefits Class and Amergis Class Member, was compromised in the Data Breach.

121. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Kelly Benefits Class and Amergis Class Members. Plaintiff's Counsel are competent and experienced in litigating class actions.

122. **Predominance.** Kelly Benefits and Amergis engaged in a common course of conduct toward Plaintiff and Kelly Benefits Class and Amergis Class Members, in that their data was stored on the same Kelly Benefits software and products and were unlawfully accessed in the same manner. The common issues arising from Kelly Benefits' and Amergis' conduct affecting Class Members listed above predominate over any individualized issues. Adjudication of these common issues in a single action will advance judicial economy.

123. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the claims of the Kelly Benefits Class and Amergis Class. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Kelly Benefits Class and Amergis Class Members would

likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Kelly Benefits Class and Amergis Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Kelly Benefits and Amergis. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Kelly Benefits Class and Amergis Class Member.

124. Kelly Benefits has acted on grounds that apply generally to the Kelly Benefits Class and Amergis Class as a whole such that injunctive relief, and declaratory relief are appropriate on a classwide basis.

125. Likewise, particular issues are appropriate for certification because such claims present common issues whose resolution would advance the disposition of this matter. Such particular issues include, but are not limited to:

- Whether Kelly Benefits and Amergis owed a legal duty to Plaintiff and Kelly Benefits Class and Amergis Class Members to protect their PII.
- Whether Kelly Benefits' and Amergis' data security measures were inadequate in light of applicable regulations and industry standards.
- Whether Kelly Benefits' and Amergis' data security measures were negligent.

126. Finally, all members of the proposed Kelly Benefits Class and Amergis Class are readily ascertainable. Both Kelly Benefits and Amergis have access to the names and contact information of Kelly Benefits Class and Amergis Class Members affected by the Data Breach.

IX. Causes of Action

A. Count I: Negligence
(On behalf of the Plaintiff and the Kelly Benefits Class and Amergis Class)

127. Plaintiff repeats and re-alleges the factual allegations above as if fully set forth

herein.

128. Kelly Benefits and Amergis owed a duty under common law to Plaintiff and Kelly Benefits Class and Amergis Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and deleting their PII in its possession from being compromised, stolen, or misused by unauthorized persons.

129. Specifically, this duty included, among other things: (a) implementing industry standard data security safeguards to protect the PII of Plaintiff and Kelly Benefits Class and Amergis Class Members; (b) maintaining, testing, and monitoring Kelly Benefits' and Amergis' security systems to ensure that PII was adequately secured and protected; (c) implementing intrusion detection systems and timely notifying customers of suspicious intrusions; (d) ensuring any third party software products to which they entrusted Plaintiff and Kelly Benefits Class and Amergis Class Member's PII were adequately and reasonably secure and was not vulnerable to exploitation; and (e) adequately notifying Plaintiff and Kelly Benefits Class and Amergis Class Members about the types of data that were compromised in the Data Breach.

130. Kelly Benefits' and Amergis' duties to use reasonable care arose from several sources, including those set out below.

131. Kelly Benefits and Amergis had a common law duty to prevent foreseeable harm to others. This duty existed because Kelly Benefits and Amergis stored valuable PII that is routinely targeted by cyber criminals. Plaintiff and Kelly Benefits Class and Amergis Class Members were the foreseeable and probable victims of any compromise to inadequate data security practices maintained by Kelly Benefits and Amergis.

132. Kelly Benefits and Amergis further assumed a duty of reasonable care in making representations in marketing materials and their respective Privacy Policies concerning data

security.

133. Kelly Benefits and Amergis breached their duty owed to the Plaintiff and Kelly Benefits Class and Amergis Class Members by failing to maintain adequate data security practices that conformed with industry standards and were, therefore, negligent.

134. Kelly Benefits and Amergis breached its duties owed to Plaintiff and Kelly Benefits Class and Amergis Class Members by failing to ensure any third-party vendor or software they used were adequately and reasonably secure to protect the PII Plaintiff and Kelly Benefits Class and Amergis Class Members entrusted to Defendants.

135. But for Kelly Benefits' and Amergis' negligence, the PII of Plaintiff and Kelly Benefits Class and Amergis Class Members would not have been stolen by cybercriminals in the Data Breach.

136. As a direct and proximate result of Kelly Benefits' and Amergis' breach of their duties, Plaintiff and Kelly Benefits Class and Amergis Class Members have suffered injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of their PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their PII.

137. As a direct and proximate result of Kelly Benefits' and Amergis' negligence,

Plaintiff and Kelly Benefits Class and Amergis Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

B. Count II: Breach of Implied Contract
(On behalf of Plaintiff and the Amergis Class)

138. Plaintiff repeats and re-alleges the factual allegations above as if fully set forth herein.

139. As a condition of employment with Amergis or participating in an assignment or engagement offered through Amergis, Amergis required Plaintiff and Amergis Class Members to provide their PII.

140. In mandating that Plaintiff and Amergis Class Members provide their PII, Amergis implied an assent to safeguard and protect their PII.

141. Plaintiff and Amergis Class Members would not have provided their PII to Amergis had they known that Amergis would not safeguard their PII as promised.

142. Plaintiff and Amergis Class Members fully performed their obligations under their implied contracts with Amergis.

143. Amergis breached its implied contracts with Plaintiff and Amergis Class Members by failing to safeguard their PII.

144. As a direct and proximate result of Amergis' breach of implied contract, Plaintiff and Amergis Class Members have suffered injuries in fact including (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of their PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (vii) nominal damages; and (viii) the continued and certainly increased risk to their

PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII.

145. As a direct and proximate result of Amergis' breach of implied contract, Plaintiff and Amergis Class Members are entitled to damages, including compensatory damages, punitive damages, and/or nominal damages, in an amount to be proven at trial.

C. Count III: Unjust Enrichment (On behalf of Plaintiff and the Kelly Benefit Class and Amergis Class)

146. Plaintiff repeats and re-alleges the factual allegations above as if fully set forth herein.

147. Plaintiff brings this Count in the alternative to Count II above.

148. Upon information and belief, Defendants fund any data security measures they implement entirely from their general revenues, including from money they make (including that supplied by contractual payments directly or indirectly by Plaintiff and Class Members) based upon representations of protecting PII.

149. Thus, there is a direct nexus between money paid to Defendants and the requirement that Defendants keep PII confidential and protected.

150. Plaintiff and Class Members paid Defendants, directly or indirectly, a certain sum of money, which was used to fund any data security measures implemented by Defendants.

151. As such, a portion of the payments made by Plaintiff and Class Members (or made on their behalf) is to be allocated to and used to provide a reasonable and adequate level of data security, the amount of which is known to Defendants.

152. Protecting PII is integral to Defendants' businesses. Without PII, Defendants would

be unable to provide the business services which comprise Defendants' core businesses.

153. Plaintiff's and Class Members' PII has monetary value. Thus, Plaintiff and Class Members conferred a monetary benefit on Defendants.

154. Defendants collected and stored the PII provided by Plaintiff and the Class to Defendants. In exchange, Plaintiff and Class Members should have received from Defendants the services that comprise Defendants' businesses and should have had the PII protected with adequate data security.

155. Defendants knew that Plaintiff and Class Members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the PII entrusted to them. Defendants profited from the PII and used the PII for business purposes.

156. Defendants failed to secure the PII and, therefore, did not fully compensate Plaintiff and Class Members for the value that the PII provided.

157. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure the PII, they would not have entrusted the PII to Defendants or obtained services from Defendants.

158. Plaintiff and Class Members have no adequate remedy at law.

159. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure the PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decisions to prioritize their own profits over the requisite data security and the safety of Plaintiff's and Class Members' PII.

160. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon them.

161. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of their PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (vii) nominal damages; and (viii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII.

162. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

163. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests

judgment against Defendants and that the Court grant the following:

A. An Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;

B. Equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. Injunctive relief, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to pay out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII, for Plaintiff's and Class Members' lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII

of Plaintiff and Class Members;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and controls so that if one area of Defendants' networks is compromised, hackers cannot gain access to portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and how to respond to a breach;

xiii. requiring Defendants to implement testing systems to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, and randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting PII;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for internal and external threats, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to unauthorized third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: May 22, 2025

/s/ Cyril V. Smith
Cyril V. Smith (Fed. Bar No. 07332)
Zuckerman Spaeder LLP
100 East Pratt Street – Suite 2440
Baltimore, Maryland 21202
Tel: 410-332-0444
Fax: 410-659-0436
csmith@zuckerman.com

James J. Pizzirusso (Fed. Bar No. 20817)
Nicholas U. Murphy
(*PHV application forthcoming)*
HAUSFELD LLP
1201 17th Street N.W., Suite 600
Washington, D.C. 20036
Tel: 202.540.7200
jpizzirusso@hausfeld.com
nmurphy@hausfeld.com